Audit Report

ALLEGATIONS TO THE DEFENSE HOTLINE ON THE
DEFENSE SECURITY ASSISTANCE MANAGEMENT SYSTEM

Report No. D-2001-141 June 19, 2001

Office of the Inspector General
Department of Defense

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 19Jun2001	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Allegations to the Defense Hotline on the Defense Security Assistance Management System	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General, Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884	**Performing Organization Number(s)** D-2001-141
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract
This audit was performed in response to nine allegations made to the Defense Hotline in February 2000 concerning management of the Defense Security Assistance Management System (DSAMS) and the Defense Security Assistance Development Center. The allegations included mismanagement of the system, inappropriate use of Government funds, and questionable use of contracted foreign national employees. (Appendix B provides a synopsis of each allegation and audit results.) The Defense Security Cooperation Agency initiated development of the DSAMS in 1995, to manage and process foreign military sales and replace 13 legacy systems. The foreign military sales program generated revenues of about $12.1 billion in FY 2000. The system was originally estimated to cost $58.3 million, to take approximately 5 years to become operational, and to have a life span of at least 10 years after becoming fully operational. In October 2000, the Director, Defense Security Cooperation Agency, cancelled two of the five modules originally envisioned for DSAMS, based on concerns raised by the agency’s Chief Information Officer.

Subject Terms

Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 44	

Additional Copies

To obtain additional copies of this report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937 or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2885

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ADP	Automatic Data Processing
BDM	BDM Engineering Services Company
DEIS	Defense Enterprise Integration Services
DISA	Defense Information Systems Agency
DSADC	Defense Security Assistance Development Center
DSAMS	Defense Security Assistance Management System
DSCA	Defense Security Cooperation Agency
FAR	Federal Acquisition Regulation
FMS	Foreign Military Sales
IG, DoD	Inspector General, Department of Defense
OSI	Office of Special Investigations
PWC	PricewaterhouseCoopers

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

June 19, 2001

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, DEFENSE SECURITY COOPERATION AGENCY
DIRECTOR, DEFENSE PROCUREMENT

SUBJECT: Audit Report on Allegations to the Defense Hotline on the Defense Security Assistance Management System (Report No. D-2001-141)

We are providing this audit report for review and comment. We conducted the audit in response to a Defense Hotline complaint. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. Comments from the Director, Defense Security Cooperation Agency and the Director, Defense Procurement, were responsive. Comments from the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) were not fully responsive. Therefore, we request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide additional comments to Recommendation A.2. by August 6, 2001.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Kimberley A. Caprio at (703) 604-9139 (DSN 664-9139) (kcaprio@dodig.osd.mil) or Mr. Dennis L. Conway at (703) 604-9158 (DSN 664-9158) (dconway@dodig.osd.mil). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Acting Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-141 **June 19, 2001**
Project No. (D-2000FG-0162)

Allegations to the Defense Hotline on the Defense Security Assistance Management System

Executive Summary

Introduction. This audit was performed in response to nine allegations made to the Defense Hotline in February 2000 concerning management of the Defense Security Assistance Management System (DSAMS) and the Defense Security Assistance Development Center. The allegations included mismanagement of the system, inappropriate use of Government funds, and questionable use of contracted foreign national employees. (Appendix B provides a synopsis of each allegation and audit results.) The Defense Security Cooperation Agency initiated development of the DSAMS in 1995, to manage and process foreign military sales and replace 13 legacy systems. The foreign military sales program generated revenues of about $12.1 billion in FY 2000. The system was originally estimated to cost $58.3 million, to take approximately 5 years to become operational, and to have a life span of at least 10 years after becoming fully operational. In October 2000, the Director, Defense Security Cooperation Agency, cancelled two of the five modules originally envisioned for DSAMS, based on concerns raised by the agency's Chief Information Officer.

Objective. The audit objective was to review the nine allegations made to the Defense Hotline and to determine whether the DSAMS was being managed to meet cost, schedule, performance, user, and security requirements.

Results. We determined that six of the nine allegations were not substantiated. Two of the three substantiated allegations involved poor program management and allowing access to the system by contractor employees, including foreign nationals, without appropriate security investigations. The remaining allegation substantiated that contractors and Government employees received training together; however, the allegation had no impact on the management of the system. As of February 2001, two of five DSAMS modules were operational and estimated costs of $83.5 million exceeded the original cost goal by $25.2 million. As originally designed, the system costs could range to $196 million and scheduled completion could extend to 13 years beyond the original completion date of 1999.

PricewaterhouseCoopers, under contract to design and develop DSAMS, hired 174 employees since 1995, including at least 38 foreign nationals, to work on the DSAMS without security investigations. As a result of not requiring security investigations until January 2000, contractor employees (foreign national and U.S. citizens) without security investigations have designed and developed the system. This increases the risk of the system, as well as other systems that interface with it, to compromise including penetration or damage that could result in a significant loss, misuse, or destruction of security assistance data. In 1997, the Air Force Office of Special Investigations conducted an investigation of foreign national employees working on the DSAMS and cited similar concerns. However, no action was taken (finding A).

We identified seven task orders awarded under a Defense Information Systems Agency "Defense Enterprise Integration Services II" contract that required contractor work on

unclassified sensitive systems. The contract did not require security investigations for contractor employees. As a result, DoD automated information systems could be vulnerable to penetration or damage that could result in high risk for loss, misuse, or destruction of data processed by the systems (finding B).

Summary of Recommendations. We recommend that the Director, Defense Security Cooperation Agency, assess the risk and benefits of continuing development of the DSAMS, and if continued, use life-cycle documents to monitor cost and schedule goals. We also recommend that the Director delay additional work on the system until security investigations are obtained and existing computer code is tested. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) identify the DSAMS as a major system and amend DoD Regulation 5200.2 to address security investigation requirements for foreign national contractor employees. We recommend that the Director, Defense Procurement, establish a Defense Federal Acquisition Regulation Supplement clause to require security investigations of contractor personnel working on or having access to DoD information systems.

Management Comments. The Director, Defense Security Cooperation Agency, concurred with revising goals for system costs and scheduled completion, performing an assessment and testing risky computer coding, and revising contract actions to require security investigations on contracted employees. The Director partially concurred with delaying work on the system until security investigations were completed on contracted employees, but stated that he was willing to accept the risk of continuing work while attempting to obtain the investigations, rather than incur additional schedule delays and costs. The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) partially concurred with identifying DSAMS as a major system. The Acting Assistant Secretary stated that additional information was being gathered to assist with making a final decision. The Acting Assistant Secretary concurred with updating the DoD security regulation to require security investigations for contractor employees with access to DoD systems. The Director, Defense Procurement stated that the problems identified did not require a new contract clause because the appropriate action was to update the DoD Regulation 5200.2-R to require security investigations for contractor employees with access to DoD systems. A discussion of management comments is in the Findings section of the report and the complete text is in the Management Comments section.

Audit Response. The comments by the Director, Defense Security Cooperation Agency, and the Director, Defense Procurement, were responsive. The comments by the Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) were partially responsive. DSAMS will manage the approximately $12.1 billion annual foreign military sales program and process sensitive information, thus DSAMS needs Office of the Secretary of Defense level oversight. We request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide comments to the final report by August 6, 2001.

Table of Contents

Executive Summary i

Introduction

Background 1
Objective 2

Findings

A. Management of the Defense Security Assistance Management System 3
B. Requirements for Security Investigations 16

Appendixes

A. Audit Process
Scope and Methodology 21
Prior Coverage 22
B. Synopsis of Allegations 24
C. Report Distribution 28

Management Comments

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) 31
Defense Security Cooperation Agency 33
Defense Procurement 37

Background

Defense Security Cooperation Agency. The Defense Security Cooperation Agency (DSCA)[1] provides direction, supervision, and oversight of security cooperation programs in support of U.S. national security and foreign policy objectives. Within this role, DSCA manages requests, approvals, funding, payments, and transfers of all foreign military sales (FMS). The Defense Security Assistance Management System (DSAMS) Program Management Office in DSCA oversees the development and maintenance of DSAMS.

DoD Initiative to Develop a FMS System. In February 1995, DSCA issued a task order under a Defense Information Systems Agency (DISA) contract to BDM Engineering Services Company (BDM) to prepare a concept for designing DSAMS. In August 1995, DSCA initiated development of DSAMS to become the DoD-wide system for managing the FMS program. From 1996 through 1998, PricewaterhouseCoopers (PWC) performed as a subcontractor for BDM, and in January 2000, DSCA awarded a follow-on task order under a General Services Administration contract directly to PWC for developing DSAMS. As of February 2001, PWC and its subcontractors continue to develop and design DSAMS. For FY 2000, the FMS program generated $12.1 billion in foreign military sales.

DSAMS was originally planned to replace 13 systems operating within DSCA and the Military Departments. According to the conceptual design document, BDM estimated total development costs of DSAMS to be $58.3 million and projected that DSAMS would be completed by 1999. DSAMS, as originally planned, consisted of the following five modules.

- The Case Development module receives and processes requests for goods and services, prepares letters of offer and acceptance including pricing, financial calculations, and payment schedules.
- The Case Implementation module performs processes from receipt of customer acceptance through the establishment of the obligation and implementation by the case manager.
- The Case Execution module will handle all functions during the life of the case such as overseeing shipments, invoices, and payments.
- The Case Reconciliation and Closure module will close books on cases by performing final balancing of payments and invoices.
- The Training module will manage tuition pricing and quotas.

As of February 2001, DSCA stated the Case Development and Case Implementation modules were operational and included over one million lines of

[1]The Defense Security Assistance Agency was renamed the Defense Security Cooperation Agency in 1998.

computer code. A computer line of code is a single statement or instruction written by a computer programmer when creating a computer program to accomplish a specific task.

Defense Hotline Referral. This audit was performed in response to nine allegations made to the Defense Hotline concerning management of DSAMS and the Defense Security Assistance Development Center (DSADC). The allegations included mismanagement of the DSAMS program, inappropriate use of Government funds, and questionable use of contracted foreign national employees.

Appendix B provides a list of the allegations and audit results that addresses seven of the nine allegations made to the Defense Hotline. To preserve the confidentiality of the complainant, we did not report on two of the allegations. The two unreported allegations (Allegations Nos. 2 and 3) were not substantiated as valid allegations and did not impact management of the DSAMS program or the security issues addressed for the contractor employees.

DoD Regulation for System Acquisition. DoD 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs," May 11, 1999, version,[2] established requirements for the acquisition and development of automated information systems. Specifically, the regulation requires that specific documents be prepared when designing or developing a system, including a mission needs statement, an operational requirements document, an acquisition program baseline, acquisition strategy, acquisition plan, and a test and evaluation master plan.

Objective

The audit objective was to review the nine allegations made to the Defense Hotline to determine whether DSAMS would meet cost, schedule, performance, user, and security requirements. Appendix A discusses the scope, methodology, management control program, and prior audit coverage.

[2]For purposes of this audit, we are using the May 1999 version. However, an interim version dated January 4, 2001 exists.

A. Management of the Defense Security Assistance Management System

The audit substantiated three of the nine Defense Hotline allegations. Specifically, as of February 2001, DSAMS had exceeded its original cost goal of $58.3 million by an estimated $25.2 million and costs were continuing to escalate. Furthermore, only two of the five modules were operational and work on two other modules had been cancelled. In addition, 174 employees that worked for PWC and its subcontractors, including at least 38 foreign nationals, have worked on DSAMS without security investigations. The allegation was also substantiated that contractors and Government employees received training together. However, the allegation had no impact on the management of DSAMS. (See Appendix B for a synopsis of the allegations and related audit results.)

The cost and schedule overruns occurred because DSCA made poor estimates on the size of the system and software development costs. In addition, PWC contractor employees, including foreign nationals, had access to DSAMS because DSCA management did not take steps to ensure that the contractual agreements with PWC included security restrictions or required security investigations.

As a result, if the security assistance system is designed and developed, as originally planned, the system could incur costs ranging to $196 million and not become fully operational until 2012, which is 13 years beyond its originally scheduled completion date. In addition, foreign national employees from countries involved in economic espionage, information warfare, and collection of military intelligence were involved in designing and developing parts of DSAMS. Therefore, the risk is increased that DSAMS, as well as other systems that interface with DSAMS, could be vulnerable to compromise, including penetration or damage that could result in a significant loss, misuse, or destruction of security assistance data supporting the FMS program, which for FY 2000 generated approximately $12.1 billion in foreign military sales.

Managing the Development of Foreign Military Sales Systems

DSCA has experienced prior problems managing the development of its FMS systems. For example, DSCA initiated a 5-year project in 1983 to develop a new FMS accounting system at a cost of $45 million. However, by December 1987, the cost of the system had increased to $75 million. In June 1988, a House Committee on Government Operations report stated that the "(FMS) system was in shambles," and that DoD lacked the controls needed to ensure that the FMS accounting system was properly managed. The report further recommended that project management be overhauled and that further development proceed using a streamlined design process. Subsequently, on July 1, 1988, the Deputy Secretary of Defense canceled the FMS accounting system.

History of the DSAMS Program. In 1995, DSCA initiated the development of DSAMS. As originally planned, DSAMS was to replace 13 systems used by the Military Departments and DSCA, and to be completed within 5 years.

In Inspector General (IG), DoD, Report No. 98-095, "Defense Security Assistance Management System," March 24, 1998, we evaluated DSCA progress in developing DSAMS. We reported that DSAMS was not being managed with controls appropriate for a system of its cost and size. Specifically, the report noted that DSAMS lacked acquisition documents such as a mission needs statement, an operational requirements document, a program baseline, an acquisition strategy, an acquisition plan, and a test and evaluation master plan as required by DoD Regulation 5000.2-R.

Further, the IG, DoD, report recommended that DSCA prepare an overall acquisition strategy for DSAMS to manage user requirements, that DSAMS be declared a major automated system by the DoD Chief Information Officer, and that the acquisition documents be completed. In response to our recommendation, the DSAMS Program Management Office developed a series of documents in accordance with DoD Regulation 5000.2-R, including an acquisition program baseline. The acquisition program baseline included goals for program cost, schedule, and expected performance. The acquisition program baseline is helpful in analyzing deviations from the approved goals, such as schedule goals.

Cost and Schedule of DSAMS Program

Regulations Related to Cost, Schedule, and Performance. DoD Directive 5000.1, "Defense Acquisition," March 15, 1996, requires program managers and users of systems to develop goals for expected cost, schedule, and performance of a system. The program manager should refine these goals as the system is developed. These goals should then be compared with actual system performance to ensure that a system will be affordable, timely, and operationally effective. These goals and system performance measures help program managers effectively manage the design and development of a system, such as DSAMS.

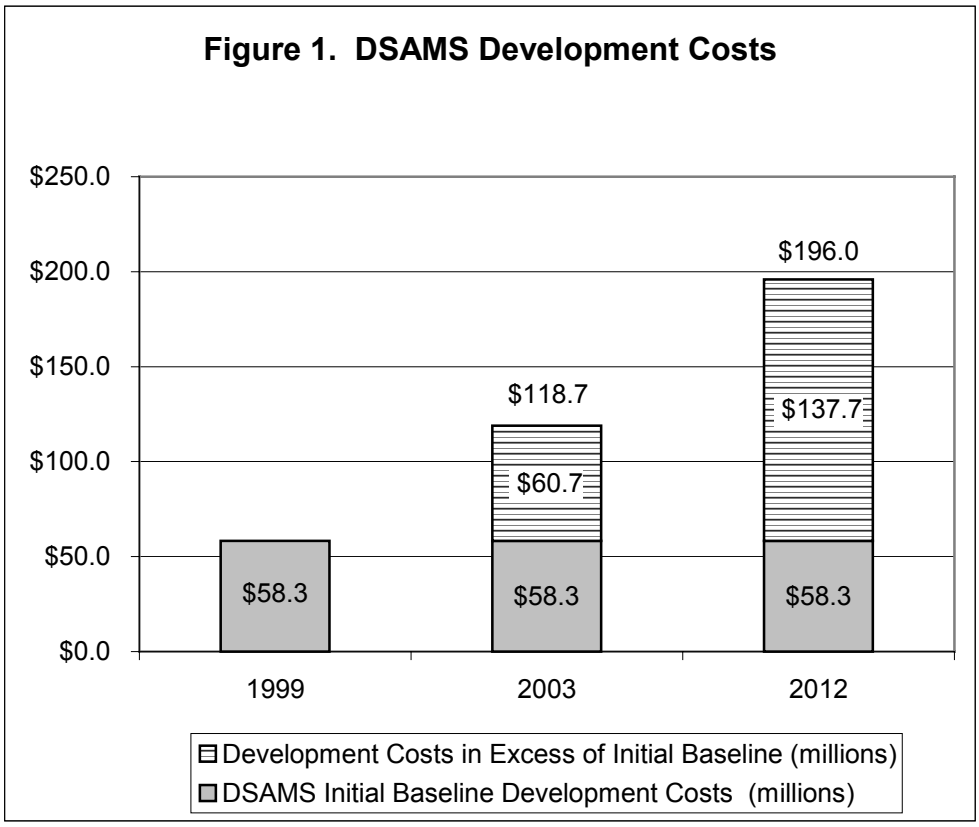
Estimated Cost of DSAMS. DSCA officials had difficulty estimating and documenting DSAMS costs. In 1995, the DSAMS Program Management Office originally estimated DSAMS development costs to be $58.3 million through 1999. As no acquisition program baseline was developed at this time, the $58.3 million was considered as the initial baseline cost.

In February 1998, the acquisition program baseline for DSAMS (which was not developed until September 1998 as a result of an IG, DoD report) showed that estimated development costs had increased to $118.7 million and the scheduled completion date had changed to 2003. In July 2000, the Chief Information Officer, DSCA, estimated development costs ranging up to $196 million by 2012. The $196 million estimate represents an increase of $137.7 million over the initial baseline development costs of $58.3 million, and $77.3 million over the re-baselined development cost estimate of $118.7 million. The Chief Information Officer attributed the cost increases to poor estimates on the size of the system and software development costs made by the DSAMS Program Management Office.

Between February 1999 and October 2000, as a result of the poor estimates, the Chief Information Officer advised the Director, DSCA, that costs would exceed the baseline. As a result of the concerns, the Director, DSCA, re-evaluated DSAMS, and in October 2000, cancelled two of the remaining three modules and began considering other alternatives.

Figure 1 presents the estimated cost growth between 1999 and 2012, based on current development cost estimates.

Figure 1. DSAMS Development Costs



In August 2000, the DSAMS Program Manager estimated costs to be $83.5 million through FY 2000, which was $25.2 million over the original 1995 cost goal of $58.3 million. However, the program manager stated that the $83.5 million was only an estimate and could not provide documents supporting the actual costs or the $83.5 million. Because the DSAMS program manager could not provide the actual development costs incurred by the DSAMS program or documentation to support the estimated $83.5 million of costs for DSAMS, the true cost of the DSAMS program could not be determined.

DSAMS Completion Schedule. In 1995, DSCA contracted with BDM to perform a study to develop a DSAMS conceptual design. The study concluded that DSAMS was achievable and would incur development costs of $58.3 million by its scheduled completion in 1999. Also, based on the results of the study, the DSAMS Program Management Office estimated that the five DSAMS modules would be completed and fully operational by 1999.

The February 1998 acquisition program baseline for DSAMS showed that the scheduled completion date would slip from 1999 to 2003. However, by November 1999, the Program Management Office estimated that the completion date for DSAMS would slip to 2005. The Chief Information Officer, DSCA, attributed the schedule escalation to poor estimates on the size of the system and software development requirements. In addition, the DSAMS Program Manager stated that the contractor needed additional time to rework design and interface problems.

Concerns Over Cost Growth and Schedule Slippage. In 1999, the Chief Information Officer, DSCA, raised concerns regarding cost and schedule escalations. As of July 2000, the Chief Information Officer realized that completion of DSAMS would slip to 2012, which was 13 years beyond the original goal of 1999. The Chief Information Officer computed this increased estimate for completing the remaining three modules based on the time required to complete the initial two modules. Using this information, in conjunction with the fact that estimated costs were exceeding the initial baseline by as much as $25.2 million and could exceed the baseline by as much as $137.7 million, the Director, DSCA, in October 2000, decided to cancel work on two of the three remaining system modules to control the escalating costs.

While DSCA managers had taken these actions, as of February 2001 only two of the five modules were operational. Further, estimated costs exceeded the original cost goal of $58.3 million by an estimated $25.2 million and scheduled completion had slipped beyond the original goal of 1999. In addition, the costs and alternatives associated with performing the tasks of the cancelled modules had not been determined.

Use of Foreign Nationals

In addition to cost and schedule increases, 174 contractor employees, including at least 38 foreign nationals, have worked on DSAMS without having their trustworthiness determined from security investigations.

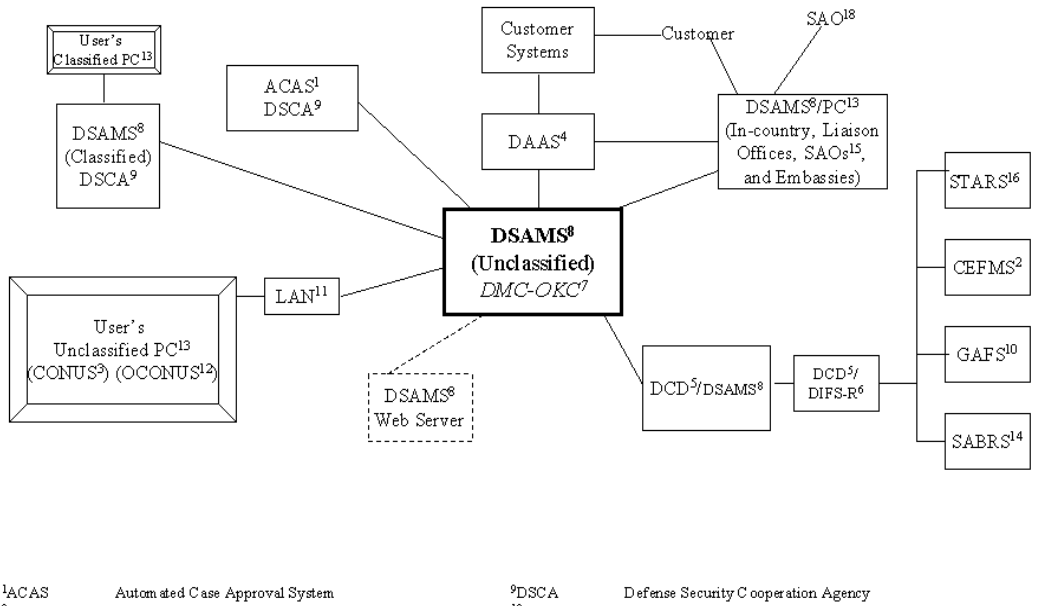
Sensitivity of DSAMS Information. DSAMS was originally planned to manage FMS information to include processing requests for major defense armaments, repair parts, and training in U.S. military schools or by mobile training teams. FMS also includes construction, contract administration, program management, technical support, and repair of equipment. Also, DSAMS was originally planned to process invoices, shipments, and payments; and perform final balancing of payments and invoices for a sale.

Of the 174 contractor employees, we determined that at least 20 of the 38 foreign national employees, hired by PWC and its subcontractors, worked in positions that allowed exposure to sensitive functions in DSAMS. For example, PWC hired 3 foreign national employees as system architects to design DSAMS and 17 foreign

nationals as computer programmers to develop the system. By virtue of these positions, these employees had direct access to and knowledge of DSAMS design and development, as well as potential access to other DoD systems.

Figure 2 presents the planned interfaces between DSAMS and other DoD systems.[3] While DSAMS was planned to process unclassified information, personnel with access to DSAMS could inappropriately use DSAMS as a way to enter other DoD systems, if adequate controls between the systems are not in place.

Figure 2. DSAMS Systems Interface Chart



[1]ACAS	Automated Case Approval System	[9]DSCA	Defense Security Cooperation Agency
[2]CEFMS	Corps of Engineers Financial Management System	[10]GAFS	General Accounting and Finance System
[3]CONUS	Continental U.S.	[11]LAN	Local Area Network
[4]DAAS	Defense Automated Addressing System	[12]OCONUS	Outside Continental U.S.
[5]DCD	Defense Corporate Database	[13]PC	Personal Computer
[6]DIFS-R	Defense Integrated Financial System - Reengineered	[14]SABRS	Standard Accounting, Budgeting, and Reporting System
[7]DMC-OKC	Defense Mega Center – Oklahoma City	[15]SAO	Security Assistance Office
[8]DSAMS	Defense Security Assistance Management System	[16]STARS	Standard Accounting and Reporting System

Some of the PWC and subcontractor foreign national employees were from countries reported to be involved in economic espionage, information warfare, and the collection of military intelligence. According to DoD Regulation 5200.2-R, "Personnel Security Program," January 1987, some of these employees should have been categorized as working in "critical-sensitive positions" and needed security investigations prior to working on DSAMS. This is significant because individuals

[3]The Standard Accounting and Reporting System; the Corps of Engineers Financial Management System; the General Accounting and Finance System; and the Standard Accounting, Budgeting, and Reporting System are DoD's primary accounting systems.

that design computer software or have access to a computer during its operation or maintenance also pose a high risk for causing grave damage or obtaining significant personal gain if protection between systems is inadequate.

Security Restrictions for DSAMS Employees. Prior to January 2000, DSCA did not require PWC to determine the trustworthiness of PWC and subcontractor employees working on DSAMS by requesting security investigations. The original task order awarded to BDM in 1995 did not require security investigations, nor did the task order awarded to PWC in January 2000. No security investigations were initiated prior to January 2000 because the DSAMS program manager considered DSAMS to be an unclassified system, and therefore no security restrictions were necessary. In addition, DSCA assumed that DISA would ensure that all contractual requirements were met including any security requirements because the task order was assigned to a DISA contract. According to DISA, the initiator of a task order, and not DISA (the contracting office), should specify any unique requirements including security requirements desired in a task order. (See finding B for additional information.)

Qualifications of PWC Employees. From December 1995 through January 15, 2001, PWC and its subcontractors hired at least 174 contractor employees, including at least 38 foreign national employees, to work on DSAMS. Based on information provided by PWC in January 2001, we determined that 10 of 174 employees had clearances, but we were unable to obtain the information from PWC that would have identified the type of security investigation associated with the clearances for these 10 employees or the date the security investigations were performed. Consequently, we were unable to determine whether any of the 174 employees had security investigations prior to starting work on DSAMS. As of February 2001, DSCA still had not finalized any of the security investigations. The absence of security investigations represents a failure to comply with DoD Regulation 5200.2-R requirements. We were unable to determine the number of BDM employees that worked on DSAMS from 1996 to 1999 without security investigations.

Table 1 identifies the citizenship of the 174 employees that had worked for PWC or its subcontractors as of December 2000. As of January 2001, PWC was unable to provide documentation on the nationalities of 65 employees.

Table 1. Citizenship of Contractor Employees

Contractor	U.S. Citizens	Foreign Nationals	Citizenship Unknown	**Total**
Pricewater-houseCoopers	51	22	46	**119**
Subcontractors	20	16	19	**55**
Total	**71**	**38**	**65**	**174**

Risks Related to Security Investigations. The risk incurred when hiring employees to perform sensitive functions without requiring security investigations was clearly addressed in a U.S. Senate report, "Investigating the Year 2000 Problem: The 100 Day Report," September 22, 1999. The report concluded that foreign national employees without security investigations were allowed extensive access, influence, and control of U.S. software. Further, many of the foreign national employees allowed to work on the Year 2000 technology problem were from countries actively pursuing information warfare capabilities against the United States and the intelligence agencies within those countries were closely tied with their economic sectors. Specifically, the report cited significant risks with allowing untrustworthy personnel the opportunity to:

- design "trap doors"[4] that allow intruders to gain undetected access to a computer network or to proprietary and sensitive information;
- develop malicious code that can destroy hardware and software, deny and disrupt access, or include Trojan horses;[5] and
- inflict long-term consequences of foreign intelligence collection, espionage activity, reduced information assurance, a loss of economic advantage, and an increase in key infrastructure vulnerability.

Further, the report stated that these risks compound the fact that no automated way exists to scan for malicious code or trap doors. (A trap door can be placed into a system using as little as four lines of code. If a trap door is inserted into network software, an adversary could gain access for years without detection.)

To reduce the risk of a system being designed and developed that was vulnerable to economic espionage, information warfare, and intelligence collection actions, the DSAMS Program Management Office needed to ensure security investigations were conducted on contractor employees to determine their trustworthiness.

Nationalities of Contractor Employees. Table 2 identifies the nationalities of the 38 foreign national employees known to have worked for PWC and its subcontractors since 1996.

[4]A trap door is an entry point into the security of a system deliberately placed by system developers.

[5]A Trojan horse is a destructive program disguised as a harmless program.

Table 2. Nationalities of Foreign National Employees[6]					
Country	Economic Espionage	Information Warfare	Pricewaterhouse Coopers	Sub-Contractor	Total
Russia	Yes	Yes	11	0	**11**
China	Yes	Yes	2	7	**9**
India	Yes	Yes	3	4	**7**
Ukraine	No	No	4	0	**4**
Taiwan	No	No	1	1	**2**
Korea	No	No	0	1	**1**
Bulgaria	Yes	Limited	0	1	**1**
Sri Lanka	No	No	0	1	**1**
Vietnam	No	No	0	1	**1**
Unknown	-	-	1	0	**1**
Totals			**22**	**16**	**38**

Special Investigation on Foreign National Employees. In 1997, the Air Force Office of Special Investigations (OSI) conducted an investigation into the use of foreign national employees for DSAMS. The Air Force OSI cited serious concerns with foreign national employees designing and developing DoD information systems without security investigations. The concerns were elevated to the Deputy Director, DSCA. However, the Deputy Director, DSCA, chose to take no action to remedy the concerns and the Air Force OSI closed the case without further actions. DSCA personnel stated that no actions were taken in response to the concerns in the 1997 investigation report because DSCA considered DSAMS to be an unclassified system.

According to DoD Instruction 5240.4, "Reporting of Counterintelligence and Criminal Violations," September 22, 1992, DSCA managers should have reported the counterintelligence issues presented in the Air Force OSI to the Secretary of Defense. As of February 2001, DSCA had not met this requirement.

Studies Conducted on DSAMS. DSCA conducted studies during the audit to assess the adequacy of security controls and the design of DSAMS. The results of

[6] Economic espionage and information warfare data were presented in the U.S. Senate Report "Investigating the Year 2000 Problem: The 100 Day Report," September 22, 1999. The U.S. Senate report was prepared by the U.S. Senate Special Committee on the Year 2000 technology problem.

these studies indicate weaknesses that could make the system more vulnerable to misuse by uninvestigated foreign national employees allowed to design and develop DSAMS.

PWC Independent Study on Security Controls. Concurrent with our initiating an audit in April 2000, DSCA hired PWC[7] to independently perform a security review of DSAMS and to identify and assess the adequacy of security controls over DSAMS. The purpose of the PWC review was to identify vulnerabilities that could be exploited by personnel working for DSCA or its contractors. The PWC report, issued in September 2000, cited 53 specific findings for enhancing the security of DSAMS. Of the 53 findings, 7 were considered "high risk" or significant weaknesses, to include the following.

- DSAMS users could potentially gain control of a transaction from its beginning to completion with no involvement or subsequent review by other parties, increasing the risk of inappropriate actions.

- DSAMS "superusers" could gain control of a transaction from its beginning to completion with no involvement or review by other parties. The fact that these "superusers" were not regularly monitored further increased the risk of unauthorized access and modification to data. ("Superusers" are high-risk individuals because they are typically the most knowledgeable about a computer system. With such high-level access and their knowledge of the system, "superusers" have the ability to perform any function or change any data in DSAMS.)

Albion International Study on DSAMS Design. DSADC is responsible for maintaining DSAMS. To assess its responsibilities, DSADC contracted with Albion International in April 2001 to perform a technical assessment of DSAMS, including DSAMS architecture and code. Albion International issued a draft report on May 10, 2001. DSCA is currently developing comments in response to the report.

Attempts to Obtain Investigations. In January 2000, the Chief Information Officer, DSCA, asked PWC to send requests to the Defense Security Service for security investigations. In March 2000, PWC submitted the names of 16 foreign nationals working on DSAMS for security investigations. The Defense Security Service did not approve these requests because DSCA had not provided justification stating that the access was critical to the national security. In June 2000, PWC resubmitted the requests; however, as of February 2001, the 15 investigations completed by the Defense Security Service were still not adjudicated by DSCA.

IG, DoD Report on Defense Security Service. In IG, DoD Report No. D-2000-111, "Security Clearance Investigative Priorities," April 5, 2000, we reported that DoD lacked assurance that personnel in mission-critical and high-risk positions will receive timely security clearances because DoD has been unable to prevent major delays in the investigative process. As a result, programs would be operationally impacted and subjected to a higher risk of compromise. According to the report,

[7]The PWC Assurance and Technology Risk Services teams that performed the security review were independent of the PWC management consulting group that was contracted to design DSAMS.

DoD will require 2 million investigations by the end of FY 2001, with an average of 137 to 262 days to close an investigation (depending on the level of clearance required).

Management Actions Taken

On October 18, 2000, the DSCA, Chief Information Officer stated that the Director, DSCA, was briefed on the significant cost growth associated with developing and fielding the DSAMS Case Execution Module and the Case Reconciliation and Closure module. Based on this information, the Director, DSCA, cancelled all development work on these modules and directed that other alternatives be considered. Other alternatives include, for example, assessing the potential of modifying existing security assistance systems or developing new modules. According to a DSCA publication on DSAMS, a draft Mission Needs Statement for a new Case Execution Module was approved by a Senior Steering Group on May 30, 2001. In addition, the Director, DSCA, stated that DSCA would continue contracting for the Training Module. According to the DSCA, Chief Information Officer, regardless of how DSAMS evolves, the DoD military security assistance commands will continue to need the functionality of all five modules.

With regard to security requirements, DSCA recognized that DSAMS was an "unclassified-sensitive" system, and therefore, security requirements should be incorporated into the contract with PWC. DSCA initiated a modification to the contract in January 2001; however, as of February 2001, the modification had not been signed.

Acquisition Baseline

Return on Investment. DoD Regulation 5000.2-R requires an analysis of alternatives for the acquisition of information systems and states that a key factor in deciding between alternatives is the return on investment. Further, the "DoD Automated Information System (AIS) Economic Analysis Guide User's Manual," May 1, 1995, requires a return on investment of 1.1 for information systems (that is, $1.10 should be received as a benefit in return for every $1.00 invested).

In November 1998, the DSCA, Chief Information Officer, estimated a return on the resources invested in DSAMS of .77. In July 2000, the Chief Information Officer recalculated the return on investment to be .86. Both of the returns on investment fell well short of the minimum requirement of 1.1. Continuation of the DSAMS program at the current rate of cost growth and schedule slippage is unlikely to result in achieving the goal of a return on investment greater than 1.

Actions Needed. The Director of DSCA recognized the program cost growth and schedule slippage and the need to incorporate security requirements into contracted efforts. However, we remain concerned regarding the slippages, in addition to the vulnerabilities inherent in the two completed modules because of the lack of security investigations of contractor employees, including foreign national employees who designed, programmed and developed the completed modules. We are concerned,

in particular, that the issue of a lack of security investigations renders DSAMS susceptible to economic espionage, information warfare, and collection of military intelligence. Further, the system has an increased vulnerability to penetration or damage that could result in the loss, misuse, or destruction of security assistance data supporting over $12.1 billion of FMS in FY 2000.

Until a decision is made on how to satisfy managing FMS, the total cost and a date for full operational capability will not be known. Furthermore, until DSCA reduces the additional risk of using in excess of one million lines of computer code written for DSAMS which have not been independently verified and validated, the system remains vulnerable to loss, misuse, or destruction.

The Director, DSCA, needs to assess the risk of continuing development of DSAMS in light of the cost, schedule, and security issues. If continued development is deemed appropriate, the Director, DSCA, should minimize risk by updating and using life-cycle documents to reestablish a baseline for cost and schedule goals. In addition, the Director, DSCA, should perform an independent risk assessment of DSAMS to identify any of the lines of code that are considered at risk and test such computer code already completed in the two operational system modules as well as any code developed prior to obtaining security investigations of contractor employees developing and designing DSAMS. Further, the Director of DSCA should include security investigations on contractor and subcontractor employees in all future contract actions for DSAMS, as well as consider the delay of any further work on DSAMS until the security investigations are obtained by PWC and existing code is tested.

DoD Oversight. According to DoD Instruction 5000.2, "Operation of the Defense Acquisition System," October 23, 2000, a system can be classified as a major automated information system of special interest to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) even though the system does not meet the dollar thresholds of a major automated information system. A special interest system requires Office of the Secretary of Defense oversight because of its importance to the DoD mission, its high development, operating, or maintenance costs, or its significant role in the administration of DoD programs.

DSAMS is important to the DoD mission because it is planned to be the single DoD-wide system for managing the foreign military sales program. In addition, the development costs for DSAMS, as originally planned, could exceed $196 million. Regardless of the level of program development costs, however, DSAMS will play a major role in the administration of the FMS program because it will manage the FMS program which for FY 2000 generated $12.1 billion in foreign military sales. Consequently, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) should initiate oversight of DSAMS.

Recommendations, Management Comments, and Audit Response

A.1. We recommend that the Director, Defense Security Cooperation Agency assess the risk of continuing development of the Defense Security Assistance Management System. If development is continued, take the following actions to minimize risk:

a. Reestablish a baseline for life-cycle documents to manage cost and schedule goals.

Management Comments. The Director, Defense Security Cooperation Agency concurred and stated that a revised baseline was approved December 11, 2000, and projected a cost for completing the training module at $30 million through December 2003.

b. Perform an independent risk assessment of the system to identify any of the lines of code that are considered at risk of being compromised.

Management Comments. The Director, Defense Security Cooperation Agency concurred and stated that an independent validation of potentially malicious code would be performed but not until contractor trustworthiness determinations are completed. The Defense Security Cooperation Agency plan is to wait until security investigations on all contractor employees have been completed and approved, then perform an independent code review. In the interim, the agency planned to transfer all code maintenance to the Defense Security Assistance Development Center by May 31, 2001.

c. Test all lines of code identified as being at risk.

Management Comments. The Director, Defense Security Cooperation Agency concurred and stated the requirement has been that all at-risk code would be re-tested.

d. Revise all present and future Defense Security Assistance Management System contract actions to require security investigations on contractor and subcontractor employees.

Management Comments. The Director, Defense Security Cooperation Agency, concurred and stated that the requirement has been in place since early 2000 and that appropriate language was incorporated as part of the contract renewal awarded on April 16, 2001.

e. Delay any additional work on the Defense Security Assistance Management System until security investigations are obtained by contractor employees and existing computer code is tested.

Management Comments. The Director, Defense Security Cooperation Agency partially concurred with this recommendation. The Director acknowledged that it was desirable to complete contractor investigations prior to starting work on the

Defense Security Assistance Management System, but that delaying further work on the system would result in a loss of specialized and knowledgeable contractor employees as well as increase costs. Further, investigative backlogs at the Defense Security Service could result in an indeterminate delay. The Defense Security Cooperation Agency approach was to complete development of the Training module and contain the risk while simultaneously completing the investigations on the contractors and conducting independent code reviews. This is a tradeoff between business objectives, costs, and risks. Further, in the absence of evidence of an actual security problem, as distinct from the increased risk of one, the Director elected to accept the risk.

Audit Response. We consider the comments to Recommendations A.1.a. through A.1.e., to be responsive. The Director has made a decision to continue development and we have pointed out the risks. Although we may not totally agree, this is a management decision.

A.2. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) identify the Defense Security Assistance Management System as a major system and provide Information Technology-Overarching Integrated Product Team oversight.

Management Comments. The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) partially concurred and stated that they were gathering facts and holding preliminary discussions to determine whether the Defense Security Assistance Management System should be designated a major automated system based on dollars to be invested or as a special interest system. The Acting Assistant Secretary stated that he planned to hold an Integrated Product Team meeting within 30 days, with Office of the Inspector General personnel present, to address oversight. If issues cannot be resolved at that level, issues in dispute may be elevated.

Audit Response. We consider the comments to be partially responsive. We believe the Defense Security Assistance Management System is important to the DoD mission because it will manage the foreign military sales program, which was $12.1 billion in FY 2000, and process sales transactions that can affect sensitive relationships between the U.S. and foreign countries. Therefore, we believe that, at a minimum, the system should be designated for special interest oversight regardless of the dollar threshold. We request that the Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide additional comments to the final report.

B. Requirements for Security Investigations

Contractor employees were working on DoD automated information systems under a Defense Information Systems Agency contract prior to receiving security investigations. These employees were allowed to work on DoD systems because DoD activities were not ensuring the task orders under the contract included requirements for investigating these employees. As a result, the DoD automated information systems were vulnerable to penetration or damage that could result in high risk for loss, misuse, or destruction of data processed by the systems.

Contract Employees Working on DoD Systems. We performed a review of task orders issued against the DISA "Defense Enterprise Integration Services II" (DEIS II) contract. The DEIS II contract is an indefinite delivery, indefinite quantity contract for information technology services and is available for use by DISA and other DoD activities. The contracts for DSAMS with BDM and PWC were originally obtained by DSCA issuing task orders against the DEIS II contract.[8]

Because we identified that DSCA did not ensure that the task orders addressed security requirements for DSAMS which processes "unclassified, but sensitive" information, we expanded our review of DEIS II task orders beyond those awarded by DSCA. Based on a limited review of task orders, we concluded that contractor employees were working on other DoD automated information systems, in addition to DSAMS, without requiring security investigations.

Personnel Security Requirements. DoD Regulation 5200.2, "Personnel Security Program," January 1987, prescribes security requirements for both Government and contractor personnel that work on DoD systems. The regulation classifies automated information system positions into three categories based on the sensitivity of the functions performed. The categories are Automatic Data Processing (ADP) I, ADP II, and ADP III. Each category requires, at a minimum, a security investigation according to the sensitivity of the functions performed. The regulation requires that even employees categorized as "non-sensitive" receive a National Agency Check or an Entrance National Agency Check prior to working on DoD systems.

- **ADP I.** Employees assigned to the most sensitive or "critical-sensitive positions" require a background investigation to include a review of personnel records and interviews with sources of information. These employees normally design computer software or access a computer system during its operation or maintenance with a high risk for causing grave damage or obtaining significant personal gain.

- **ADP II.** Employees assigned to "non-critical sensitive positions" require only a Defense National Agency Check with written inquiries or a National

[8]In January 2000, DSCA awarded the DSAMS work to PWC under a General Services Administration contract rather than the DEIS contract.

Agency Check with written inquiries.[9] Employees assigned to "non-critical sensitive positions" would be responsible for directing, planning, designing, operating, or maintaining an information system.

- **ADP III.** Employees not assigned to positions considered "critical-sensitive" or "non-critical sensitive" are classified as "non-sensitive." Personnel in non-sensitive positions require, at a minimum, a National Agency Check or an Entrance National Agency Check.

DEIS II Review. As of December 19, 2000, we identified a total of 590 DEIS II task orders. We selected 364 task orders, awarded from September 30, 1997 through November 8, 2000, for review and determined that 52 of the 364 task orders did not require security investigations. Of the 52 task orders, 7 task orders specified that the systems processed "unclassified, but sensitive" information, while 45 task orders specified that "unclassified" information would be processed.

The 52 task orders related to 14 DoD information systems. We further determined that 7 of the 14 DoD systems were identified as critical systems according to the Information Technology Registration Database maintained by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). A critical system is an information system that is vital to the operation of an activity and the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency. The seven critical systems were as follows:

- Global Combat Support System,
- Support Equipment Resources Management Information System,
- Standard Depot System,
- Distribution Standard System,
- Asset Tracking for Logistics and Supply System,
- Worldwide Port System, and
- Transportation Operational Personal Property Standard System.

Of the seven task orders related to systems that process "unclassified, sensitive" information, none of those systems are considered critical. However, it is highly probable that some of the currently non-critical systems will become critical systems at a future date because they contain sensitive data. For example, one of the non-critical systems is the Wide-Area Workflow, a system that is under development at present. Wide-Area Workflow is a key element in the DoD end-to-end procurement

[9]A Defense National Agency Check with written inquiries is a security investigation conducted by the Defense Investigative Service for determining the trustworthiness of personnel. This security investigation includes a National Agency Check, credit bureau check, and written inquiries to current and former employers. A National Agency Check with written inquiries is a security investigation conducted by the Office of Personnel Management that consists of a National Agency Check combined with written inquiries to law enforcement agencies, former employers, and supervisors.

process and will facilitate receipt and acceptance functions. As such, once fully operational, it may become a critical system. Other systems that may become critical include the Joint Defense Infrastructure Control System, the Integrated Logistics System, and the Past Performance Automated Information System.

Contractual Requirements for Security Investigations. Based on the review, we concluded that contractor employees were allowed to work on DoD systems, in addition to DSAMS, prior to having security investigations. This occurred because DoD activities were not ensuring contracts included requirements for investigating these employees. In the case of DSAMS, DSCA officials stated that they assumed that since the task order was placed on a DISA contract, DISA would ensure all contractual requirements were met, including any security requirements. However, according to DISA, it is the responsibility of the activity initiating the task order, and not DISA to specify any unique requirements including security requirements. The DISA assertion is supported by DoD Regulation 5200.2, in that activities are required to ensure that Government and contractor personnel working on DoD systems receive security investigations based on the sensitivity of the functions performed. As such, DoD activities should ensure contractor employees have security investigations prior to working on DoD systems.

Implications of Lack of Security Investigations. The lack of security investigations of Government and contractor personnel make DoD systems vulnerable to penetration or damage that could result in a high risk for loss, misuse, or destruction of data processed by critical DoD systems. We did not perform work to determine the existence of security investigations for employees contracted to work on the 52 task orders under the DEIS II contract. However, the concerns cited in this report regarding the vulnerability of DSAMS to economic espionage, information warfare, and collection of military intelligence, demand that DoD activities review task orders and comply with personnel security requirements for contractor employees.

Security Issues Identified in Prior IG, DoD Reports. Following Year 2000 renovations to DoD systems, the IG, DoD, performed an audit to determine user adherence to DoD information systems security policy during and after Year 2000 renovation efforts. IG, DoD, Report No. D-2001-016, "Security Controls Over Contractor Support for Year 2000 Renovation," December 12, 2000, cited concerns regarding security controls over contractor personnel having access to DoD systems to make Year 2000 renovations. DoD Components used techniques such as access controls, configuration management, and code verification and validation, to monitor and control contractor access to the 159 mission-critical systems sampled for the report. However, according to DoD Components, only 134 of the 159 contractor renovated systems had access controls and personnel security background checks were completed for only 121 systems. Because DoD Components did not always implement access controls or verify that background checks for the contractors were complete or up to date, the effectiveness of the access control was diminished. We recommended that the Chief Information Officers for DoD Components assess the risk to renovated systems and reaccredit as necessary.

In addition, IG, DoD, Report No. D-2000-130, "Foreign National Access to Automated Information Systems," May 26, 2000, stated that the Army and Navy

did not have adequate procedures for authorizing and controlling access by foreign nationals to information available on automated information systems and local area networks. As a result, at least 126 foreign nationals had unrestricted access to automated information systems and local area networks. As a result, the foreign nationals could gain unauthorized access to militarily sensitive technologies and other controlled information systems and local area networks at Army and Navy facilities. We recommended that the Army and Navy revise applicable regulations to ensure foreign national visitors cannot gain access to militarily sensitive technologies. The Office of the Director of Information Systems for Command, Control, Communications, and Computers concurred with the recommendation, but lacks purview over the Military Departments.

Responsibility for Personnel Security. DoD Directive 5200.2, "DoD Personnel Security Program," April 9, 1999, states that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) has the responsibility, as the DoD senior agency official, for the personnel security program. This responsibility includes establishing policy for security investigations of Government and contractor employees. Given the high risks of using contracted foreign national employees without security investigations, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) should amend DoD Regulation 5200.2-R to address security investigation requirements for foreign national contractor employees.

While the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), is responsible for personnel security policy, within DoD, the Director, Defense Procurement, is responsible for contracting policy. In that role, the Director, Defense Procurement, is responsible for presiding over the Defense Acquisition Regulation Council which oversees and coordinates changes to the Defense Federal Acquisition Regulation Supplement. As such, to ensure that contracting officers are aware of and include the requirement for security investigations in contracts for information technology, the Director, Defense Procurement, should establish a clause in the Defense Federal Acquisition Regulation Supplement to implement the requirement for security investigations as defined in DoD Regulation 5200.2-R.

Recommendations, Management Comments, and Audit Response

B.1. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) amend DoD Regulation 5200.2 to address security investigation requirements for foreign national contractor employees working on or having access to DoD information systems.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), concurred with this recommendation. The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that a proposed policy change updating DoD Regulation 5200.2-R has been developed requiring uniform investigative and adjudicative requirements for all contractor employees to include foreign nationals.

This change in policy will be ready for coordination by June 2001 and a published change to DoD Regulation 5200.2-R made by October 2001.

B.2. We recommend that the Director, Defense Procurement, in conjunction with the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), establish a requirement in the Defense Federal Acquisition Regulation Supplement, to implement the requirement for security investigations of contractor employees working on or having access to DoD information systems, as defined in DoD Regulation 5200.2.

Management Comments. The Director, Defense Procurement, nonconcurred with this recommendation. The Director stated that the action by the Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to change DoD Regulation 5200.2-R was the appropriate response to ensure investigative and adjudicative policy for determining trustworthiness of all contractor employees.

Audit Response. We consider the comments to be responsive. The responsibility for determining the need to ensure sufficient investigative and adjudicative steps are taken for contractor employees is the responsibility of the procuring activity. As such, the action by the Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to change DoD Regulation 5200.2-R should be appropriate for determining the trustworthiness of all contractor employees.

Appendix A. Audit Process

Scope and Methodology

Work Performed. We performed audit work to examine complaints alleged by a Defense Hotline complainant in February 2000. Specifically, we examined nine allegations made concerning management of the DSAMS program.

We interviewed the complainant, the DSAMS program manager, the Chief Information Officer, DSCA, the DSCA Comptroller, the DSCA Contracting Officers Technical Representative, the DSCA security officer, and the Deputy Director of the Defense Security Assistance Development Center (DSADC). We also interviewed personnel in the DISA foreign military sales office and the PWC project management office for DSAMS and the Defense Acquisition Regulations Directorate. We reviewed data provided by these managers to determine if the acquisition management process was followed, acquisition documents were updated, and if personnel security investigations were performed. Also, we evaluated the allegations concerning mismanagement of the DSAMS program costs and schedule, and the use of contractor employees to design and develop DSAMS that did not have security investigations. We also obtained and reviewed information provided by contractors and the Air Force OSI. We did not review the management control program because the audit was limited to only a review of the hotline allegations.

DSCA manages DSAMS and provides direction, supervision, and oversight of security cooperation programs in support of U.S. national security and foreign policy objectives. In August 1995, DSCA began developing DSAMS to become the worldwide system for managing the approximately $12.1 billion FMS program.

DoD-Wide Corporate-Level Government Performance and Results Act Coverage. In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. Although the Secretary of Defense has not established any goals for Information Technology Management, the General Accounting Office lists it as a high-risk area. This report pertains to Information Technology Management as well as to achievement of the following goal and subordinate performance goal:

- **FY 2001 DoD Corporate-Level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(01-DoD-2)**

- **FY 2001 Subordinate Performance Goal 2.5:** Improve DoD financial and information management. **(01-DoD-2.5)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals:

- **Information Technology Management Functional Area. Objective:** Ensure DoD's vital information resources are secure and protected. **Goal:** Build information assurance framework. **(ITM-4.1)**

- **Information Technology Management Functional Area. Objective:** Ensure DoD's vital information resources are secure and protected. **Goal:** Assess information assurance posture of DoD operational systems. **(ITM-4.4)**

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Information Technology Management high-risk area.

Use of Computer-Processed Data. We did not use computer-processed data for this audit.

Audit Type, Dates, and Standards. We performed this program results audit to investigate a Defense Hotline complaint from July 2000 through February 2001 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did our work in accordance with generally accepted government auditing standards except that we were unable to obtain an opinion on our system of quality control. The most recent external quality control review was withdrawn on March 15, 2001, and we will undergo a new review.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Prior Coverage

During the past 3 years, the Inspector General, DoD, has issued four audit reports discussing DSAMS and foreign national employees access to information systems, as follows:

Inspector General, DoD, Report No. D-2001-016, "Security Controls Over Contractor Support for Year 2000 Renovation," December 12, 2000

Inspector General, DoD, Report No. D-2000-130, "Foreign National Access to Automated Information Systems," May 26, 2000

Inspector General, DoD, Report No. D-2000-111, "Security Clearance Investigative Priorities," April 5, 2000

Inspector General, DoD, Report No. 98-095, "Defense Security Assistance Management Systems (DSAMS)," March 24, 1998

Appendix B. Synopsis of Allegations

The audit was conducted to investigate a complaint, consisting of multiple allegations, made to the Defense Hotline on the management of DSAMS. We summarized the complaint into nine allegations, as follows.

Allegation No. 1: The DSAMS program experienced mismanagement regarding cost, schedule, and performance.

> **Audit Results.** Allegation substantiated. DSAMS experienced substantial cost growth and schedule slippage. The estimated cost of the DSAMS program increased from $58.3 million in FY 1995 to $83.5 million in FY 2000. Furthermore, DSCA could not fully support the life-cycle costs for DSAMS, could not tell what the actual costs spent to date were, and DSAMS could slip 13 years from a planned completion date in FY 1999 to FY 2012. Management of these risks is required by DoD Regulation 5000.2-R (Interim), "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," October 23, 2000, and mandated by the Clinger-Cohen Act of 1996 to assure that risks are mitigated.
>
> To minimize costs for the current DSAMS program, the Director, DSCA, canceled the development of the Case Execution Module effective October 18, 2000.
>
> The allegation also suggested, but was not substantiated, that key DSCA officials covered up DSAMS failures.

Allegation Nos. 2 and 3: To preserve the confidentiality of the complainant, we are not reporting on Allegations Nos. 2 and 3. These two allegations were not substantiated as being valid and did not impact management of the DSAMS program or the security issues addressed for the contractor employees.

Allegation No. 4: Personnel from PWC wrote the DSAMS statement of work, bid on the project, and DSCA subsequently awarded the DSAMS contract to PWC.

> **Audit Results.** Allegation not substantiated. PWC had been a subcontractor under a contract awarded to BDM Engineering Services Company in FY 1995. In January 2000, DSCA awarded PWC a 5-year contract, renewable annually. The Federal Acquisition Regulation (FAR) 9.505-2, "Preparing Specifications for Work Statements," June 6, 2000, explains that a contractor may write a statement of work only if that contractor has participated in the development and design work. Therefore, based on the FAR this allegation is not confirmed.

Allegation No. 5: Six Russian nationals designed and programmed DSAMS but were not allowed entry onto a DoD installation.

Audit Results. Allegation substantiated. Russian citizens employed by PWC were not allowed entry onto a Navy installation at Mechanicsburg, Pennsylvania. More than six Russian citizens had been used by PWC for the DSAMS project. PWC actually used at least 38 foreign nationals to develop DSAMS whose trustworthiness had not been determined through proper security investigations. The foreign nationals included personnel from Russia, Ukraine, People's Republic of China, Pakistan, and India. As of January 2001, PWC has 17 foreign nationals assigned to the DSAMS project and none of these employees' trustworthiness has been determined through security investigations.

In 1997, the Air Force OSI conducted an investigation on foreign nationals working on the DSAMS project. The OSI concluded that there were serious concerns having foreign nationals working on DoD automated information systems that had not had their trustworthiness determined. The OSI report also noted that a PWC official had hired the foreign nationals for economic reasons because foreign nationals would work for less money than U.S. citizens. DSCA took no action on the OSI report findings, thereby failing to comply with DoD Regulation 5200.2-R, "Personnel Security Program," January 1987, by not requiring security investigations be completed on foreign nationals. Also, DSCA failed to comply with DoD Instruction 5240.4 because it did not report concerns presented in the Air Force OSI report to the Secretary of Defense. The initial failure to comply with DoD Regulation 5200.2-R had allowed foreign national employees to work on DSAMS that had not received a security investigation. Many of these foreign nationals worked on critical parts such as development and system architecture.

Allegation No. 6: Contractor employees received training with Government employees at Government expense.

Audit Results. Allegation substantiated. However, it had no impact on the management of DSAMS. Government and contractor employees were receiving training together. The current contract does not specify who will pay for this training. It was indeterminable, however, which law or directives DSCA or PWC had violated by having joint training. Regardless, the training of Government and contractor employees together does maximize the training dollar and expands the knowledge base.

Allegation No. 7: Contractor employees assigned work directly to Government employees.

Audit Results. Allegation not substantiated. Both Government employees and contractor employees are on teams to strengthen the development process of DSAMS. As problems arise during module development, team members generate trouble process reports. On some occasions contractor employees do generate trouble process reports and Government employees correct the deficiencies. Contractor employees are not performing inherently Government functions. An inherent Government function as defined by Office of Management and Budget

Circular A-76, "Performance of Commercial Activities," August 4, 1983 (Revised 1999), is one that is so intimately related to the public interest as to mandate its performance by Government employees. These functions include those activities which require the exercise of discretion in applying Government authority, or the use of value judgment in making decisions for the Government. The method employed at DSADC by teaming Government employees and contractor employees together assures that the greatest amount of expertise is brought to bear on the development of DSAMS.

Allegation No. 8: DSADC lacked a separate DSADC-specific strategic plan.

Audit Results. Allegation not substantiated. The Government Performance and Results Act requires agencies to develop strategic plans. DSADC is currently included as an independent appendix to the DSCA Strategic Plan. There is no benefit to have a DSADC specific Strategic Plan separate from the DSCA Strategic Plan. DSCA is the parent unit and DSADC is subordinate to it. Consequently, it is quite natural for the parent organization to have a consolidated strategic plan with its constituent parts as independent appendixes.

Allegation No. 9: DSADC circumvented the DoD Priority Placement Program. Specifically, job announcements were listed as temporary, but in some cases made permanent without further competition. In addition, at least 80 percent to 90 percent of DSADC employees inappropriately received at least a one-grade promotion circumventing the DoD Priority Placement Program.

Audit Results. Originally, the allegation was substantiated; however, local officials reversed an improper decision to service DSADC as a downsizing organization for priority placement purposes, and therefore no remedy was needed.

DoD established DSADC by merging similar departments from the Services' security assistance commands. In many cases the grade structure approved at DSADC was higher at DSADC than at the Services' security assistance commands. Consequently, DSADC management felt it necessary to offer promotions to the employees transferred from the Services' security assistance commands to DSADC to retain an experienced knowledge base.

In researching and preparing to make the promotion offers, DSADC management coordinated with its supporting Human Resources Office, a Navy function located at Mechanicsburg, Pennsylvania. This human resources office chose to service DSADC as an organization that was downsizing. This allowed the servicing human resources office to apply Navy policy to the DSADC request for promotions. This decision effectively allowed all promotion notices to carry a statement that the positions were temporary but could become permanent within 1 year. As a result, the subsequent job announcements were exempt from the DoD Priority Placement Program, as downsizing agencies and organizations are exempted from the DoD Priority Placement Program. However, once the regional Human Resources Office at Philadelphia,

Pennsylvania became aware of the decision rendered by the Mechanicsburg Human Resources Office (about 9 months later), the regional office advised the Mechanicsburg office that it had made an incorrect decision. Consequently, the Mechanicsburg Human Resources Office reversed its decision and DSADC job announcements are no longer exempt from the DoD Priority Placement Program.

During the period that the Mechanicsburg Human Resources Office allowed the DSADC to be exempted from the DoD Priority Placement Program, about 56 employees had received promotions. Fifteen of these promotions were because of accretion. The DoD Priority Placement Program manual states that accretions are exempt from the Priority Placement Program. The impact of the remaining 41 positions to the DoD Priority Placement Program is unknown.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Acquisition, Technology, and Logistics)
  Director, Defense Procurement
Under Secretary of Defense (Policy)
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense for Security and Information Operations

Department of the Army

Commander, U.S. Army Security Assistance Command
Auditor General, Department of the Army

Department of the Navy

Director, Navy International Programs Office
Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Deputy Under Secretary of the Air Force International Affairs
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Security Cooperation Agency
Director, Defense Information Systems Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

May 10, 2001

MEMORANDUM FOR DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE, OIG

SUBJECT: Draft Audit Report on Allegations to the Defense Hotline on the Defense Security Assistance Management System (Project No. D2000FG-0162), March 20, 2001

We appreciate the opportunity to comment on the subject draft report.

For the two recommendations requiring action by the ASD (C3I), we partially concur with one and concur with the other. We partially concur with the first recommendation to identify the Defense Security Assistance Management System (DSAMS) as a major system and provide oversight through the Information Technology Overarching Integrated Product Team (IT OIPT). However, some of the acquisition-related information and recommendations in both this draft audit report and the 1998 DoDIG DSAMS Audit Report are in dispute. At this point, we are still gathering facts and have not made a decision regarding DSAMS oversight. We concur with the second recommendation to update the DoD Regulation 5200.2 to include a uniform investigative and adjudicative policy for determining trustworthiness for access by all contractors, including foreign nationals, to unclassified but sensitive DoD IT systems.

Thank you for the opportunity to review and comment on the report. The professionalism and the level of cooperation between my staff and yours are appreciated and we look forward to working with you again in the future. Should you have additional questions, please contact my action officer, William May, (703) 602-0980 extension 158 or william.may@osd.mil.

Linton Wells II
Acting

Attachment

ASD(C3I) COMMENTS

"Allegations to the Defense Hotline on the Defense Security Assistance Management System," dated March 20, 2001 (Project No. D2000FG-0162)

RECOMMENDATIONS

RECOMMENDATION A.2: DoD Inspector General (DoDIG) recommends that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) identify the Defense Security Assistance Management System (DSAMS) as a major system and provide Information Technology-Overarching Integrated Product Team oversight (IT OIPT).

ASD(C3I) RESPONSE: Partially concur. ASD(C3I)/Deputy Chief Information Officer (DCIO) staff has held preliminary discussions with Defense Security Cooperation Agency (DSCA) and DoDIG staff to determine whether DSAMS should be overseen as an Acquisition Category (ACAT) IAM Program (i.e., a Major Automated Acquisition System). Some of the acquisition-related information and recommendations in both this draft audit report and the 1998 DoDIG DSAMS audit report are in dispute. At this point, we are still gathering facts and have not made a decision regarding DSAMS oversight. The central issue is whether DSAMS crosses ACAT IA dollar thresholds, and, if not, should it be designated ACAT IA due to its potential special interest to ASD (C3I).

Our plan is to hold, within the next 30 days, an Integrated Product Team (IPT) meeting (at the Action Officer level) at which the DSAMS Program Manager will brief the Office of Secretary of Defense (OSD) and Joint Staff oversight staff, with DoDIG staff present. If DSAMS oversight issues can be resolved at that level, we will decide whether to designate DSAMS as an ACAT IA program. If the IPT is unable to resolve the issues in dispute, then subsequent meetings, perhaps at the IT OIPT level, or higher, may be necessary.

RECOMMENDATION B.1: DoDIG recommends that ASD(C3I) amend DoD Regulation 5200.2 to address security investigations for foreign national contractor employees working on or having access to DoD information systems.

ASD(C3I) RESPONSE: Concur. The C3I Security Directorate has been working on this issue for the past year and has developed a draft policy which updates the current DoD Regulation 5200.2 with regards to a uniform investigative and adjudicative policy for determining trustworthiness for access by all contractors, including foreign nationals, to unclassified but sensitive DoD IT systems. It is anticipated that this proposed policy change will be out for coordination by June 2001 and in place by October 2001.

Defense Security Cooperation Agency

DEFENSE SECURITY COOPERATION AGENCY

WASHINGTON, DC 20301-2800

MAY 4 2001

In reply refer to:
I-003952/01

MEMORANDUM FOR DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE,
DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Draft Audit Report, Project No. D2000FG-0162

Thank you for the opportunity to provide comments on the Draft DoDIG Audit Report "Allegations to the Defense Hotline on the Defense Security Assistance Management System", Project No D2000FG-0162, subject report. I appreciate the diligence of your investigators in working with us to establish a correct chronology of events.

Although I am in essential agreement with the major findings of the report, the context should be taken into consideration. For example, despite the acknowledged shortcomings in cost expectations, schedule forecasting, and personnel security practices, it is important to emphasize that two DSAMS modules have already been successfully deployed at over 70 sites throughout DoD; Military Department Case Development legacy systems have been completely shut down; and DSAMS has been a key part of DoD's Security Assistance business toolset for nearly two years. As the report notes, DSCA management was cognizant of, and actively addressing, the shortcomings prior to the Hotline complaint.

To strengthen its information technology management, in October 1998, DSCA hired a Chief Information Officer (CIO). The CIO initiated new DSAMS cost forecasts to get a more accurate picture of potential program cost. Alternatives for restructuring the program were formulated. My predecessor's office was directly involved in the decision-making process. These and other remedial measures, including reassessment of the business case, commenced prior to the Hotline allegation.

The Draft notes that numerous programs in DoD have inadequately vetted foreign nationals who lacked background investigations to support a trustworthiness determination. In January 2000, after DSCA's CIO read the prior Air Force Office of Special Investigations report, he prohibited the hiring of additional foreign national contractor employees. The contractor was required to promptly start the background investigation process for all its employees. These actions were also taken prior to the Hotline complaint. It should be emphasized that no malicious code has been detected and that development efforts on DSAMS are shared among contractor and DSCA developers.

Finally, when I became aware of the potential cost of the last DSAMS module (Case Execution, including Case Closure), I decided to cancel it. Consequently, the total development cost for DSAMS will never reach $196M. Any new development of Case Execution functionality will be conducted using a completely different approach, in full

accordance with all applicable directives, and only after the need for such a development has been revalidated.

I fully or partially concur with all of the recommendations addressed to DSCA. However, some of the key statements cited in the report require correction. First, the report makes reference to $83.5M as being the actual development costs through FY2000. That figure includes operations and maintenance; the actual program development cost through FY2000 was $74M. Second, the report cites the 1995 initial baseline cost ($58.3M) and schedule (1999) estimates in numerous places, including a chart showing estimate growth. However, the DoDIG acknowledges elsewhere in the report that DSCA re-baselined the cost ($118.7M) and schedule (2005), and DSCA reported these independent estimates to the DoDIG in 1998. Therefore, references to exceeding the original schedule and cost goal by $25.2M are inappropriate.

In light of my decision to cancel the Case Execution Module (including Case Closure), I partially concur with a recommendation assigned to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)). Our response to each of the Draft's recommendations for DSCA and ASD(C3I) is in Attachment 1.

TOME H. WALTERS, JR.
LIEUTENANT GENERAL, USAF
DIRECTOR

RESPONSE TO DoDIG RECOMMENDATIONS

A.1: We recommend that the Director, Defense Security Cooperation Agency assess the risk of continuing development of the Defense Security Assistance Management System. If development is continued, take the following actions to minimize risk:

Recommendation A.1.a: Reestablish a baseline for life-cycle documents to manage cost and schedule goals.

Comment: Concur

DSCA developed a revised baseline for development of the Training Module, the last major module in DSAMS. That baseline was presented to me and approved on December 11, 2000. It forecasts completion of the Training Module in December 2003 at a projected cost-to-completion of $30M. Cost, schedule, and requirements will be more carefully tracked to give greater in-progress visibility. The last half of the originally planned DSAMS program - the Case Execution Module (including Case Closure) – has been cancelled.

Recommendation A.1.b: Perform an independent risk assessment of the system to identify any of the lines of code that are considered at risk of being compromised.

Comment: Concur

An independent validation of code that could potentially be malicious will be performed. However, this validation should not occur until contractor trustworthiness determinations are completed. DSCA's approach, launched in January 2000, is to vet all contractors and then conduct an independent code review. In the interim, DSCA is transferring all maintenance of production code in-house at the Defense Security Assistance Development Center. This transfer will be completed on 31 May 2001.

Recommendation A.1.c: Test all lines of code identified as being at risk.

Comment: Concur

DSCA agrees that all at-risk code should be retested. DSCA has developed automated regression testing so that most code is retested prior to each DSAMS release, of which there are several per year. This practice is already in place.

Recommendation A.1.d: Revise all present and future Defense Security Assistance Management System contract actions to require security investigations on contractor and subcontractor employees.

Attachment (1)

Comment: Concur

This requirement has been in place since early 2000. Appropriate language was incorporated as part of the contract renewal that was awarded on 16 April 2001

Recommendation A.1.e: Delay any additional work on the Defense Security Assistance Management System until security investigations are obtained by contractor employees and existing computer code is tested.

Comment: Partially concur

While ideally it is desirable to complete contractor background investigations prior to commencing work, the penalties of so doing are extremely high in this case. Software development is a knowledge-intensive process. This DoDIG recommendation would result in the loss of specialized and knowledgeable contractor analysts, designers, programmers, and testers. Moreover, given the delays due to the investigation backlog in the Defense Security Service, this is a recommendation for indeterminate delay. Consequently the cost and schedule of the program would grow even more. This issue was explicitly considered in the deliberations leading to my decision to proceed to completion of the Training Module with all deliberate speed and then stop the DSAMS program. Essentially DSCA's approach is to complete development of the DSAMS Training Module and contain the risk at that point, while simultaneously vetting the contractors and conducting independent code review thereafter. This is admittedly a trade-off between business objectives, costs, and risks. But in the absence of evidence of an actual security problem, as distinct from the increased risk of one, I have elected to accept the risk.

A.2 We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) identify the Defense Security Assistance Management System as a major system and provide Information Technology-Overarching Integrated Product Team oversight.

Comment: Partially concur

Such oversight is not currently appropriate since, with the cancellation of the Case Execution Module (including Case Closure), DSAMS has already entered its final phase. DSAMS is already on the ASD(C3I) list of special interest systems and the program has been providing quarterly status reports to ASD(C3I) since 30 April 1998. Moreover, as a result of the cancellation, this program will clearly remain below major automated information system status. If and when DSCA proceeds with a major development for Case Execution, DSCA will notify ASD(C3I) and request the appropriate oversight processes be established in accordance with DoD regulations.

Defense Procurement

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION AND TECHNOLOGY

MAY 8. 2001

DP(DAR)

MEMORANDUM FOR DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE, DOD/IG

THROUGH: DIRECTOR, ACQUISITION RESOURCES AND ANALYSIS 5/14/01

SUBJECT: Draft Audit Report on Allegations to the Defense Hotline on the Defense Security Assistance Management System (Project No. D2000FG-0162), March 20, 2001

This responds to your request for comments on recommendation B2 of the draft audit report. You recommend that the Defense Federal Acquisition Regulation Supplement (DFARS) be revised to implement the requirement for security investigations of contractor employees working on or having access to DoD information systems, as defined in DoD Regulation 5200.2.

We do not believe that the problems identified require a new contracting regulation or contract clause. We believe this is a requirements issue and that the appropriate action is the one recommended to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), namely to update the DoD Regulation 5200.2 guidance to include a uniform investigative and adjudicative policy for determining trustworthiness for access by all contractors, including foreign nationals, to unclassified but sensitive DoD information technology systems.

Thank you for the opportunity to comment on the draft report.

Deidre A. Lee
Director, Defense Procurement

Audit Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector, General, DoD, who contributed to the report are listed below.

Paul J. Granetto
Kimberley A. Caprio
Dennis L. Conway
Stanley J. Arceneaux
Marcia L. Ukleya7
Michael T. Stokes
Jason E. Alt
Kim Y. Deal
Lisa Rose-Pressley